Republic of the Philippines
NATIONAL POLICE COMMISSION
PHILIPPINE NATIONAL POLICE
ANTI-CYBERCRIME GROUP
Camp BGen Rafael T Crame, Quezon City

ACG-CYBER SECURITY BULLETIN NR 280

ACG-CSB 010923280

Reference Number ACG-CSB 010923280

Be Wary of Uniform Resource Locator (URL) Manipulation Attack

The following information was obtained from different cyber security sources for notification to all parties concerned pursuant to the mandate of the Philippine National Police Anti-Cybercrime Group (PNP ACG) and classified as “Restricted” pursuant to the PNP Regulation 200-012 on Document Security and Impact Rating as high based on PNP Information Communication Technology (ICT) Security Manual s.2010-01 p. 22 and p.129.

SUMMARY

Uniform Resource Locator (URL) manipulation, also called URL rewriting is the process of altering often automatically by means of a program written for that purpose the parameters in a URL. URL manipulation can be employed as a convenience by a Web server administrator, or for nefarious purposes by a hacker. An example of the constructive use of this technique is allowing an Internet user to access a Web site that has a complicated URL by entering a simpler URL into the address bar of a Web browser.

The URL manipulation redirects the request, so the user does not have to remember, manually enter, or meticulously cut and paste a long, peculiar character string. An example of malicious URL manipulation is its implementation, without the knowledge of the affected server administrator or Internet user, for the purpose of redirecting user requests from a legitimate site to an illegitimate site. The bogus site may then install rogue code on the user's hard drive.

URL manipulation occurs when an application embeds user input into the path or domain of URLs that appear within application responses. An attacker can use this vulnerability to construct a link that, if visited by another application user, will modify the target of URLs within the response. It may be possible to leverage this to perform various attacks.

When a hacker looks to manipulate a URL, they usually change parts of the URL to test access. Since most users navigate a website through traditional means that they use the links provided on the website, sometimes hackers can find vulnerabilities by a trial-and-error approach.

By manipulating the parameters to try different values, hackers can test directories and file extensions randomly to find the resources they are after. This provides access to resources that typically would not be available and would otherwise be protected. Hackers have tools that allow them to automate these penetrations, making it possible to test a website and more specifically, find vulnerabilities in

seconds. With this method, these hackers can try searching for directories that make it possible to control the site, scripts that reveal information about the site, or for hidden files.

Editing a URL can reveal private information or allow users to perform actions which should be restricted. Manipulating a URL may reveal a private webpage. A public website may not have a link to the page, or the page may be only accessible under certain conditions.

Trust in user-side, data and inappropriate validation can lead to manipulation of data by malicious users, and consequent serious problems in cyber-attacks. The problem of data manipulation in both user side and data transmission between user and server. It provides a detailed understanding of URL manipulation attack and make a comparison between various attack methods.

To secure a web server against URL manipulation attacks, it is necessary to keep a watch on vulnerabilities and regularly apply the patches provided by the web server's publisher. Moreover, a detailed configuration of the web server helps keep users from surfing on pages they are not supposed to have access to.

RECOMMENDATION

The public are advised to follow these tips in order to prevent URL manipulation attack:

- Install anti-malware software;
- Back-up regularly and keep a recent backup copy off-site;
- Disable the display of files present in a directory that does not contain an index file;
- Update systems regularly;
- Delete unnecessary script interpreters;
- Prevent HTTP viewing of HTTPS accessible pages; and
- Delete unnecessary configuration options.

For additional information, please refer to the following websites:

- https://www.techtarget.com/whatis/definition/URL-manipulation-URL-rewriting
- https://cits.technology/blog/why-is-url-manipulation-a-security-concern
- https://ccm.net/security/viruses/10087-url-manipulation-attacks/

POINT OF CONTACT

Please contact **PMAJ JUN-JUN S DAGURO** Police Community Relations Officer thru e-mail address acg@pnp.gov.ph or contact us on telephone number (632) 723-0401 local 7483 for any inquiries related to this CYBER SECURITY BULLETIN.